Date: Wed, 17 Aug 94 04:30:24 PDT
From: Ham-Digital Mailing List and Newsgroup <ham-digital@ucsd.edu>
Errors-To: Ham-Digital-Errors@UCSD.Edu
Reply-To: Ham-Digital@UCSD.Edu
Precedence: Bulk
Subject: Ham-Digital Digest V94 #274
To: Ham-Digital

Ham-Digital Digest Wed, 17 Aug 94 Volume 94 : Issue 274

Today's Topics:

Send Replies or notes for publication to: <Ham-Digital@UCSD.Edu>
Send subscription requests to: <Ham-Digital-REQUEST@UCSD.Edu>
Problems you can't solve otherwise to brian@ucsd.edu.

Archives of past issues of the Ham-Digital Digest are available
(by FTP only) from UCSD.Edu in directory "mailarchives/ham-digital".

Date: 16 Aug 1994 17:53:42 GMT
From: ihnp4.ucsd.edu!news.cerf.net!mvb.saic.com!MathWorks.Com!yeshua.marcam.com!
zip.eecs.umich.edu!newsxfer.itd.umich.edu!ncar!newshost.lanl.gov!beta.lanl.gov!
wolf@network.ucsd.edu
Subject: 900MHz phone spread spectrum systems
To: ham-digital@ucsd.edu

here's the summary of relevant details that arose from my earlier post
requesting details on the 900 MHz ss phones. i was somewhat dismayed;
very few seemed to have any hard facts on these systems. i tried to
sort out the conflicting info, so some of this may not yet be right.
hopefully someone in the know will enlighten us.

i had asked:

" does anyone have any details on the ss systems used in, say, the escort

phones? spreading sequence generator, moduation methods, synchronization schemes, etc.? one of the felows that i talked with at cincinnatti microwave suggested that their phones choose a spreading sequence randomly whenever the phone gets used. is this true? "

it turns out that there are at least two digital schemes for 900 MHz phones. the second, not ss, is what the tropez phone uses. first i'll point out what appear to be open questions, then i'll summarize the tropez and then move on to the ss phones. finally, i'll note the cryptographic security and attack issues that were mentioned and end with some micellaneous items.

Open Questions:

what is the spreading sequence mechanism? details?
how is the sprerading sequence and digitized audio used?
audio sampling rate?
spreading sequence rate?

for the tropez, there are similar questions, though the modulation is not ss.

chip-set details?

Tropez

one poster suggested:

>>p.s. There are reports that the audio is transmitted in the clear on 450
>>MHz. Not sure of the signal level, tho.
>>
>
>yes... I reported this late last week... and am still researching it. My
>phone though, is the Tropez 900 DL which is not spread-spectrum but
>digitally modulated on single carriers within the 900 MHz band. What I
>have found is that there is some leakage of in-the-clear audio in the
>430 MHz amateur band from the handset. Others have found and reported
>similar signals. I am trying to get someone from VTech (the manufacturer
>of the phone) to discuss this with me... but they seem to be having trouble
>returning my calls.

thus it appears that the tropez does not use ss, and that there is a low level 430MHz or thereabouts (what is the exact frequency?) analog leak from the phone.

the same poster gave some details on the tropez phone's digital system:

>I believe the modulation is PCM... and it is scrambled with a one of
>64K possible patterns that is chosen each time the handset is removed
>from the base...

what is the pattern generation mechanism? how is it in some sense "randomized".
one guess would be that there is a continuously generated pseudorandom sequence
and that the time that you start to use the phone determines the phase of the
sequence relative to the start time... this would be a silly sort of rng tho.
but it would _suffice_ since it is not too difficult to design a pseudorandom
sequence generator with a short correlation length.

one would also like to know if the pseudorandom sequence bit time is long, or
short wrt the analog digitization time.

also, what is the method for using the pseudorandom noise with the digitized
audio? i.e., are the two x-or'd or something more "interesting"?

finally, if there are indeed 64K possible patterns, what generates and
determines these patterns?

another poster commented on the modulation scheme, gave a bit rate, but did
not comment on the number of pseudorandom patterns or their method of
generation:

>I'm fairly satisified with the 900 MHz Tropez I've got right now.
>It goes almost a block radius around my house. The Tropez is *not*
>spread-spectrum.. Tropez uses a single channel 16 KHz PCM signal
>that is about 100 KC wide. Unless you are in a super saturated
>location, I am not convinced that spread spectrum is significantly
>superior to the channelized units.

later they wrote, but no mention of what use is made of the "key":

>The PCM chip in the Tropez is made by Motorola. ... The CPU looks to be
>something like a 6809 derivation.
>
>The key is a 16 bit word. I don't know if there is an easy way to
>get in sync once the initial hand-shaking is done -- probably there
>is, because the system has to be farily robust in the presence of
>signal interruptions and multipath distortion.
>
>I believe the code is not sent out over the air, but is downloaded
>directly into the handset when you put the phone on the base unit.

then some comments on how the handset and base sync:

>I've noticed the base sends out a little ping when you set the the
>handset on the base. I surmised the ping does two things: 1.

>Sees if anybody else is on the same channel, if so change to
>another channel.

SS 900 MHz Systems

the folklore is that the 900 ss systems in use use direct sequence ss:

>My understanding is that these phones use direct sequence spread spectrum.

as to the synchonization scheme, the typical autocorrelation method was guessed:

>I think you sort of slide your sequence back and forth over the signal, and
>when they're synced, the signal gets clear in an easily detectable way.

and another poster said:

>Once you know the code and have the incoming signal, you can use some
>kind of sliding correlator- try the, say 63, possible starting points
>for the sequence, and find which one produces the larges received
>signal, ie the biggest correlation peak. Then you continue to lock

and a comment on "64K" codes, which i don't understand at all! whatever!
maybe someone has some actual details on the ss systems in use?

>When they say "Uses digital spread-spectrum techniques with
>64,000 different codes," they may probably be saying that there's one
>sequence and 64K access codes to dial out, which is the same as an analog
>cordless with 64K security.

another comment on the spreading sequence (?) states:

>The best US system I have heard of uses 16 bit encryption...

clearly some details are missing!

my guess is that there is a lfsr that is 16 bit wide, generating a 64K
m-sequence that is x'or'd with the digitized analog... the normal trick.

again, what is the bit rate of the prng? how many spreading sequences are
available? etc. so far we've seen no good details...

a comment on the setting of the "security code", no details on what "security
code means":

>According to the AT&T owners manual, The security code changes

>automaticly when the phone goes off hook.

one poster gave some information on the number of legally available spread-
ing sequences:

>Each Spread Spectrum user in the 900MHz range has a choice of 4
>types of spreading. I believe they are the same type as the ones allowed
>for Hams.

note: 2 lfsr schemes x 2 prng schemes = 4 types of modulation schemes. these
are the legally available ham modes.

Crypto and Security

one poster writes:

>Direct sequences are easy to figure out. (These are single shift register
>generators.) If you know how long it is, say N stages, all you need is N+1
>bits to figure out the code and the synch.

another responds:

>Strictly speaking what you say is true (and you need 2N consecutive
>bits) with two (important) conditions:
>
>   1. The shift register must be _linear_, i.e., the feedback
>   bit must be an XOR of some fixed subset of the current bits
>   of the shift register.
>
>   2. It is good to have access to the pure spreading sequence
>   _unmodulated by data_, you see, sometimes one period
>   of the spreading sequence spans more than one data bit
>   and this causes inversions.
>
>Of course, these two problems are trivial in a crypto sense. If it
>is right that they're using m-sequences (maximal length sequences)
>in these cordless phones, yes m-sequences are linear hence
>satisfy condition 1.

the second poster gets close to the issue of how to attack a ss phone
system. note that if the quiet time digitized audio spans more than
2N bits that you then have an instant "in".

is there a reference to the result mentioned?

we need details on the sppreading sequences, rates, etc. anyone have a phone and care to look up their part numbers?

another comment on security. it would appear that security is nonexistent if only a few spreading sequences are allowed, unless there is some sort of additional crypto layer in the system. note that the fcc does not allow hams to pre-encrypt their transmissions, as is suggested below.

>> Spread spectrum was not developed as an encryption scheme.
>
>Taking a wider view (no pun intended), spread spectrum is just another
>method of implementing the physical layer. If you want security,
>encrypt the digital data prior to sending it to to the DSSS
>"pseudo noise" "mixer".

Miscellaneous issues

a comment on who is making ss systems (?)

>Maxim is now offering some of the 9 GHz process technology they bought
>from Tektronix. They have a spread spectrum transmitter chip you might
>want to look at. They also have technical information about spread
>spectrum to help you.

another comment on something relevant to making listening devices ? i'm not sure what this poster intended!

>Look up companies QEI and CYLINK. Cylink is in Calf. Both about $5grand. One
>is audio only while Cylink is digital u to 500kbaud for real time video
>digital stuff. 1200 units can be on same channle AT ONCE?

one poster's thought on jamming and encryotion:

>Wasn't one of the main purposes of spread spectrum to make it
>harder to jam a signal? The encryption is just ancillary, and
>not that good? The encryption only becomes secure when you
>use a one time pad...right?a

and the response (i don't want this to become a thread on how easy it is to hide a ss system. i'm guessing that it would be very difficult given the fcc's mandate (if one poster's statement is correct) that only a few (maybe as few as two) spreading sequences be allowed.)

>Spread spectrum was not developed as an encryption scheme. The
>properties that makes it desirable are :
>

> Protection against jammers. This is measured in the AJ (anti-
> jam) ratio. Some simple math shows how much more jammer
> energy is needed to cause bit errors(digital communications)
>
> Low probability of intercept. SS signals can be placed below the
> noise floor in many cases. This means that covert operation
> can be conducted with some communications.

==========
david r wolf - wolf@lanl.gov - 1+505-667-3813 - 1+505-662-9102 -- wb4vcq
==========

Date: Mon, 15 Aug 94 21:10:17 MST
From: ihnp4.ucsd.edu!dog.ee.lbl.gov!agate!howland.reston.ans.net!swrinde!
cs.utexas.edu!asuvax!ennews!stat!david@network.ucsd.edu
Subject: [Q] best software for KAM+
To: ham-digital@ucsd.edu

khopper@kimbark.uchicago.edu (Kenneth C Hopper) writes:

> New KAM+ owner seeks good software suggestions.
> OP only on HF.

I'm running Version 9.02 of KaGold for the KAM. Been very happy with
it.

david wb7tpy

Editor, HICNet Medical Newsletter
Internet: david@stat.com FAX: +1 (602) 451-1165
Bitnet : ATW1H@ASUACAD

Date: 16 Aug 1994 15:31:59 GMT
From: ihnp4.ucsd.edu!dog.ee.lbl.gov!agate!howland.reston.ans.net!
usenet.ins.cwru.edu!cleveland.Freenet.Edu!ei938@network.ucsd.edu
Subject: AUTOEXEC.NOS for NOS with BAYCOM modem
To: ham-digital@ucsd.edu

Packet Radio Gurus:
Would an Elmer help me out of this NOS jam?

I need a copy of an AUTOEXEC.NOS file for a PA0GRI NOS configuration on my PC. I am using a BAYCOM modem (finally got that working... more details after I work out the bugs) and the AX.25 drivers for BAYCOM. I had a working copy, but during configuration/testing, it got corrupted and now it is scrambled. My backup NOS.ZIP got scrambled too, so next time I am keeping the backup on the shelf rather than on the computer.

I was trying to set the entire system up on a 1.44MB floppy disk, but it somehow did not set up correctly. I think the floppy may be on the fritz...

Can/would anyone help out and send me a copy of their AUTOEXEC.NOS for NOS with BAYCOM modem? Thank you in advance.

73!

Andrew Lynch, N8VEM
alynch@wpgate1.wpafb.af.mil

Date: 16 Aug 1994 17:15:53 GMT
From: ihnp4.ucsd.edu!agate!howland.reston.ans.net!gatech!swrinde!elroy.jpl.nasa.gov!lll-winken.llnl.gov!earl.llnl.gov!user@network.ucsd.edu
Subject: Does a FAQ exist for packet newbys?
To: ham-digital@ucsd.edu

If so, where would I find it?

Thanks,
Gary

The ramblings expressed above do not reflect the opinions of LLNL.

Gary Ross — Ross@NOVAX.LLNL.GOV
Lawrence Livermore National Laboratory — Rossman@eworld.com

NOVA Laser Operations — Rossman@aol.com
P.O. Box 808, L-489
Livermore, CA 94551

Date: 16 Aug 1994 10:31:55 -0700
From: enews.sgi.com!wdl1!ltis.loral.com!not-for-mail@decwrl.dec.com
Subject: Gateway within CA?
To: ham-digital@ucsd.edu

Is there a gateway in CA that can be used for traffic between a CA
packet address and a CA internet address? Or is gate@wb7tpy.ampr.org
the only one to be used?

Thanks for the help.
--

  hlb@ltis.loral.com

Date: Fri, 12 Aug 94 13:38:31 BST
From: pa.dec.com!csu.napier.ac.uk!ee17@decwrl.dec.com
Subject: Jnos-Enet Solved TnX !
To: ham-digital@ucsd.edu

Thanks for all the helpful replies to my problem re connecting an
ethernet packet driver to Jnos.
All sorted out now and working Tickety-Boo   :-)

PS If your ethernet is not 'flat' remember to add this to your auto.nos:

route add default <devicename> <router IP address>

otherwise you won't get off of the segment your on !!

regards and thanks again,

%% Alastair J. Downs   ____\   a.downs@csu.napier.ac.uk %%
%% E.E & Comp.Eng.Dept.   \ |\ \ \   phone +44 31 455 4389 %%
%% Napier University, Edinburgh | _   fax: +44 31 455 7938 %%
%% Scotland, UK |_| |_   GM6NEI@GB7EDN.#77.GBR.EU %%

Date: Mon, 15 Aug 1994 17:02:25 +0000
From: ihnp4.ucsd.edu!ucsnews!sol.ctr.columbia.edu!howland.reston.ans.net!pipex!
demon!myth.demon.co.uk!zeus@network.ucsd.edu
Subject: JVFAX Interfaces?
To: ham-digital@ucsd.edu

I am currently running JVFAX 5.1 (anyone know a FTP site for a more recent version?) with the simple comparator interface. Before I launch head on into building the full AM/FM serial port version, are there any plans to use the Sound Blaster ADC?, or are there any alternative circuits, since the ADC chip is proving difficult to source. Cheers.

Mike.

--

Michael S. Cowgill (Mike) _ My opinions! MINEMINEALLMINEHAHAHAHA!
zeus@myth.demon.co.uk (That's me) _ " Swirly thing alert! "
G1VOX@GB7WRG.GBR.EU 44.131.2.76 _ " ...Cracking toast Gromit!... "

Date: Mon, 15 Aug 1994 17:45:46 +0000
From: ihnp4.ucsd.edu!dog.ee.lbl.gov!agate!doc.ic.ac.uk!uknet!pipex!demon!llondel.demon.co.uk!dave@network.ucsd.edu
To: ham-digital@ucsd.edu

References <JAY.39.2E4A3859@medicine.dmed.iupui.edu>, <1994Aug12.154901.27305@ke4zv.atl.ga.us>, <32h270$12t@hpbab.mentorg.com>
Subject : Re: Packet Node Info Wanted

There seems to be a load of rubbish in this thread! While DXing to a distant BBS is usually not a good idea, on the basis that it should have the same bulls as your local one, the network should be able to handle a bit of interactive traffic between users who are several nodes apart. I have in the past had useful chats with amateurs several hundred miles away using the node system - when replies arrive in under a couple of minutes it is no problem at all.

Having said that, I can sympathise with those who maintain large chunks of the network with no support - my local network is effectively run by three people, with occasional help from a few others. There are probably 600+ users in the coverage area.

Dave
--

****
* G4WRW @ GB7WRW.#41.GBR.EU AX25   *   *
* dave@llondel.demon.co.uk Internet * Stop the World! I want to get off! *
* g4wrw@g4wrw.ampr.org   Amprnet *   *
****

Date: Tue, 16 Aug 1994 13:01:58 GMT
From: ihnp4.ucsd.edu!dog.ee.lbl.gov!overload.lbl.gov!agate!howland.reston.ans.net!gatech!wa4mei!ke4zv!gary@network.ucsd.edu
To: ham-digital@ucsd.edu

References <326vf6$dir@eagle.natinst.com>, <1994Aug9.135536.9869@ke4zv.atl.ga.us>, <1994Aug15.170956.24013@arrl.org>mei
Reply-To : gary@ke4zv.atl.ga.us (Gary Coffman)
Subject : Re: local organizations that help people get acquainted with packet radio

In article <1994Aug15.170956.24013@arrl.org> zlau@arrl.org (Zack Lau (KH6CP)) writes:
>An interesting path I've worked twice on all bands from 1.3 to
>10 GHz is Mt Equinox to Woburn, MA. While Equinox is at 3800 ft,
>there is Grand Manadnock at 3165 ft. almost in the center of
>the path (54% of the way there). On 2 meters, I need 10 watts
>and a 10 dBi antenna--with 2 watts to a 7 dBi antenna I need
>someone to relay! But, this knife edge path is workable all the
>way through 10 GHz running QRP. Path length is 179 km.

Fine, but could you guarantee a 60 db fade margin 7x24 52 weeks a year,
and no heavy multipath? That's what you need for a reliable data link
at a resonable speed (1 Mb+).

Gary
--
Gary Coffman KE4ZV | You make it, | gatech!wa4mei!ke4zv!gary
Destructive Testing Systems | we break it. | uunet!rsiatl!ke4zv!gary
534 Shannon Way | Guaranteed! | emory!kd4nc!ke4zv!gary
Lawrenceville, GA 30244 | | gary@ke4zv.atl.ga.us

End of Ham-Digital Digest V94 #274
****